ПРАКТИКИ МИНИМИЗАЦИИ ИНФОРМАЦИОННЫХ РИСКОВ В ОРГАНИЗАЦИЯХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Казберович И.Г.

Власова Г.А. – канд. техн. наук, доцент

В современном мире бурно развиваются технологии обработки, хранения и передачи информации. Применение информационных технологий требует повышенного внимания к вопросам информационной безопасности. Риск информационной безопасности организации представляет собой возможный ущерб организации в результате реализации некоторой угрозы через уязвимость. Нарушение информационной безопасности организации влечет уничтожение информационных ресурсов, недоступность либо их несанкционированное использование, что нарушает “непрерывность” бизнеса, приводит к финансовым потерям и ущербу репутации.

Для обеспечения информационной безопасности малых и средний компаний предложены следующие практики:

1. Разграничение доступа сотрудников через аутентификацию пользователей и межсетевые экраны.
2. Симуляция “фишинговых” атак для тренировки и подготовки сотрудников к подобным случаям. Согласно исследованиям компании “PhoenixNap” в 2020 году, данные атаки являются наиболее популярными среди компаний на мировом уровне.
3. Реализация удаленного доступа к корпоративной сети через VPN и использование антивирусных программ позволяют уменьшить риски атак в случае удаленной работы сотрудников.
4. Осведомленность сотрудников, удаленных сотрудников и аутсорсинговых сотрудников о конфиденциальности данных организации и их собственных данных, политиках безопасности и государственных законах путем проведения “воркшопов”, тренингов и презентаций. Согласно исследованиям Ponemon Institute, 2 из 3 атак инициируются сотрудниками и могут быть предотвращены.
5. Избежание методов социальной инженерии через sms, email, звонки, профили социальных сетей и т.д. с помощью которых получают авторизационные данные сотрудников и доступ к защищенным файлам. Сотрудники должны быть осведомлены о возможности подобных атак.
6. Внедрение подхода по управлению рисками информационной безопасности, что позволит сотрудникам оперативно определять, исследовать и реагировать на инциденты.
7. Покупка/разработка программного обеспечения по мониторингу пользовательской и файловой активности. Мониторинг пользователей позволяет легче реагировать и предотвращать инциденты.
8. Необходимо использовать менеджеры паролей (LastPass, Dashlane, CommonKey и т.д.). Использование слабых либо повторяющихся паролей одна из самых распространенных практик.
9. Периодический пересмотр списка сотрудников (особенно при увольнениях либо переходах сотрудников), имеющих привилегированный доступ к важным областям бизнеса/данным, либо разработка системы аудита привилегированных доступов.
10. Резервное копирование данных на регулярной основе.
11. Регулярные обновления и обслуживание используемых систем и обеспечения.
12. Поддержание в актуальном состоянии планов обработки рисков (информационных активов, каталогов угроз и уязвимостей и т.д.).
13. Поддержание процессов информационной безопасности в соответствии стандартам ISO, PCI, DSS, HIPAA. [1,3]

Согласно исследованиям компании “Positive Technologies” в 2019 году, из 33 организаций, протестированных на внутреннее и внешнее проникновение, популярными уязвимостями являются недостатки парольной политики, эксплуатация недостатков защиты беспроводных сетей, применение социальной инженерии и, следовательно, низкий уровень осведомленности пользователей в вопросах информационной безопасности. В результате внешнего тестирования на проникновение в 92% из 33 исследуемых компаний удалось преодолеть сетевой периметр по причине проблемы несвоевременного обновления программного обеспечения (версии прикладного ПО, серверов, веб-приложений). В результате внутренних тестов на проникновение в 100% исследуемых компаний получен контроль над внутренней инфраструктурой по причине недостаточного уровня защиты привилегированных учетных записей, словарных паролей, недостатков защиты служебных протоколов сети и хранения важной информации в открытом виде.

Для минимизации информационных рисков в организации важно следовать всем рекомендациям в комплексе, так как даже отдельные пробелы в механизмах защиты могут послужить причиной взлома инфраструктуры и компрометации критически важных ресурсов. [2]

Список использованных источников:

Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Проверка и оценка деятельности по управлению информационной безопасностью: научное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой — М.: Горячая линия-Телеком, 2013. — 166 с.

Официальный сайт компании “Positive Technologies” [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/ - Дата доступа: 04.04.2020.

Официальный сайт компании “phoenixNAP” [Электронный ресурс]. – Режим доступа: https://phoenixnap.com/blog/cybersecurity-best-practices - Дата доступа: 07.04.2020.